万水网络与安全技术丛书

黑客之道

破解黑客木马屠城计

秘密客　编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

黑客最常用的入侵手法就是透过木马程序，这些木马程序在计算机中既可以偷窃数据，又可以毁坏系统，甚至黑客可以远程控制目标计算机，面对网络上形形色色防不胜防的木马程序，我们编写了这本《黑客之道：破解黑客木马屠城计》，帮助您拦截木马程序，捍卫自己的计算机。

本书将引导您深度认识木马原理，入侵方法，提高防止黑客的战斗力，破解木马伪装与欺骗手法，让上网更安全；帮助您清除木马程序，强化电脑安全指数，将变种的木马统统揪出来斩草除根。书中讲解了 100 种抵挡木马的妙招，招招有效。

本书共分 11 章，第 1 章全面讲述了木马的基本概念，第 2 章展示了木马的危害，第 3 章教您认识伪装后的木马，第 4 章分析木马攻击的常用手段，第 5 章协助用户检测电脑是否中了木马，第 6 章指导怎样使用工具清除木马程序，第 7 章告诉我们遇到不能用工具直接清除的木马该怎样用手动方法清除该程序，第 8 章通过讲解网络资料传输的知识来加强电脑的使用安全，第 9 章全面阐述防火墙，第 10 章纵深探究木马原理，第 11 章改造木马程序为我所用。

本书适合研究黑客行为者，分析入侵行为模式、反制黑客者阅读，同时也可供研究漏洞预防御手法、杜绝与反查、提升网路安全者参考使用。

图书在版编目(CIP)数据

黑客之道：破解黑客木马屠城计 / 秘密客编著. —北京：中国水利水电出版社，2005

（万水网络与安全技术丛书）

ISBN 7-5084-2705-X

Ⅰ. 黑… Ⅱ. 秘… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 011727 号

书　　名	**黑客之道：破解黑客木马屠城计**
作　　者	秘密客　编著
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044）
	网址：www.waterpub.com.cn
	E-mail：mchannel@263.net（万水）
	sales@waterpub.com.cn
	电话：（010）63202266（总机）　68331835（营销中心）　82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16 开本　15.5 印张　350 千字
版　　次	2005 年 4 月第 1 版　2005 年 4 月第 1 次印刷
印　　数	0001—4000 册
定　　价	26.00 元

编者序

一战成名的特洛依木马，俨然已成为今日网络上最会“黑”人工具的代名词了，昔日的它身形庞大，为了隐藏众多的战士，不知得花上多少的人力物力去打造；但时至今日，为求隐身于程序或文件中，不仅在缩减体积上作文章，还学会了更多的隐身花样，吸引你我的视线，让我们在不设防的情况下误遭木马的毒手。

我们都知道黑客最常用的入侵手法就是通过木马程序，一些刚入门或想试试黑客瘾的顽皮鬼，大多使用现有的木马程序，但一些资深黑客却会根据对方系统编写专用的木马，让人防不胜防。这些驻留在计算机中的木马程序，既可以偷窃数据，又有毁坏系统的能力，甚至让黑客远程控制受害者的计算机恣意妄为，而承受这罪行恶果的“羔羊”却是倒霉的一般计算机用户。因此，为了与这股恶势力对抗，正义的一方开发出功能越来越强的防毒软件、防火墙，保护用户计算机的安全。对于这类难以正面突破的防线，黑客也有因应之道，他们制造出作用类似的木马程序，并且在一些小程序、图片或音乐文件中暗藏伏兵，诱惑不知情的计算机用户将它拉入自己的计算机中，然后就在受害者的计算机上打开后门，供黑客长驱直入、为所欲为——于是，“悲剧”就这么一出一出不停地上演。

面对网络上闹得沸沸扬扬的各式木马百变密招，您是否练就了一双“火眼金睛”，可以识破各种伪装，保护自己的计算机免于成为敌我过招下的牺牲品呢？为了协助您拦截木马程序，捍卫自己的计算机，本书将引导您深入认识木马及其入侵手法，有效防范于未然；再通过程序与鼠标的相互扶助，将木马程序赶尽杀绝；最后再从原理层面分析如何驯服木马，使其为己所用。

最终您将发现，木马程序本身无罪，罪恶之心在于滥用它的人，因此，我们需要追踪黑客木马程序，阻止伸向计算机的那只邪恶黑手！

目　　录

黑客之道：破解黑客木马屠城计

Chapter 1

揭开木马的神秘面纱——木马基本概念

“木马”在许多用户的眼中，是一个充满了神秘色彩的名词，它似乎会随时出现在联网的某台计算机，让人联想到高深莫测的黑客、网络入侵和一大堆的网络技术。但是，木马到底是什么？它有什么用途？如何分类？还有它与病毒有什么区别？黑客和木马又有着怎样的关系？面对这一连串的问题，本章将揭开木马的神秘面纱，带领大家了解木马的真实面目。

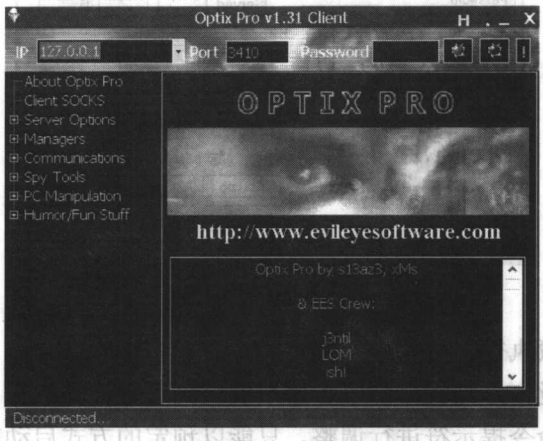
1-1 了解木马程序

木马程序也称为特洛依木马（Trojan Horse），这个名词的典故是来源于一个希腊故事。相传在公元前一千年左右，特洛依人抢走了希腊的一个王妃，于是引发了希腊与特洛依人之间的一场战争。由于特洛依城背面环山，城池坚固，希腊大军攻打了十年依然无法攻破，于是就有一名智者献计：制作一个巨大并且中空的木马塑像，里面藏着一些精锐的战士，然后烧毁自家兵营假装撤退，让特洛人将木马视为战利品带入城中之后，木马中的战士再悄悄打开城门，里应外合的攻陷特洛依城。正如智者的预料一般，当夜希腊大军攻破了特洛依城，而特洛依木马（Trojan Horse）从此成为了打开后门的代名词，专门用于指称为计算机入侵者打开方便之门的程序。

历史中的特洛依木马

1-1-1　木马的定义

在大英百科全书中，Trojan Horse 的定义是“隐藏在其他程序中的安全破坏（security-breaking）程序，如地址清单、压缩文件或游戏程序中”。从这个定义可以得知，木马程序通常不会单独出现，总是会隐藏在其他程序后面，或者以各种手段来掩护它本来的目的。



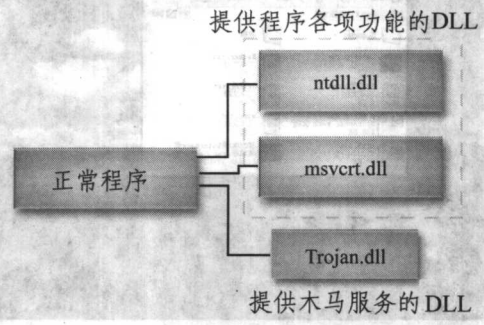
木马程序 Optix Pro 的客户端

1-1-2　木马的特征

就像病毒程序的特征是复制自己，木马程序也有它的特征，根据这些特征，用户就可以判断计算机到底是受到木马入侵，还是受到计算机病毒攻击：

- 不会通过感染文件复制自己的方式传播。

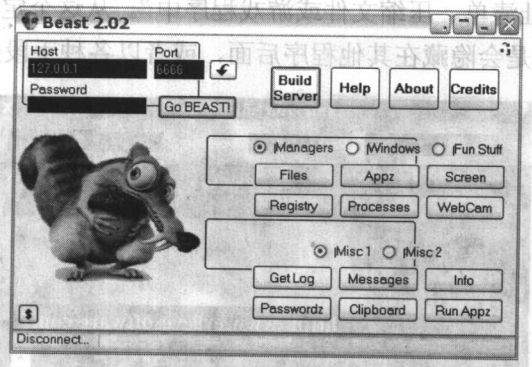
早期的木马通常以独立的执行文件的形式存在，并以程序的方式在计算机中正常执行。后来改良过的木马，则以伪装成 DLL 文件的方式，附加在其他系统文件上执行。无论哪一种木马都不会感染其他文件，并进行自我复制传播。



以 DLL 方式注册表到其他程序中的木马

- 分为客户端与服务器端两部分。

由于木马需要通过网络接收黑客的指令，所以为了能够达成互动通讯，木马需要由两部分组成。其中服务器端安装在被控制的计算机上，用于入侵系统；客户端没有入侵或破坏系统的功能，只是用于连接服务器端，并且向服务器端发送命令或通过服务器获得远程计算机的数据，客户端通常安装在黑客的计算机上。



木马 Beast 的客户端

- 服务器端隐藏执行。

为了不让用户发觉，木马程序的服务器端安装到远程计算机后，在执行时通常没有图形界面，也无法使用命令提示符进行调整。只能以预定的方式启动或执行默认的任务，如记录键盘的输入操作等等，并且开始等候客户端连接，或主动寻找客户端连接。

在工作列中看不到执行的木马服务器端程序

- 打开服务。

在被控制的计算机上打开远程文件管理，屏幕监视等功能，让黑客可以管理并控制远程计算机。

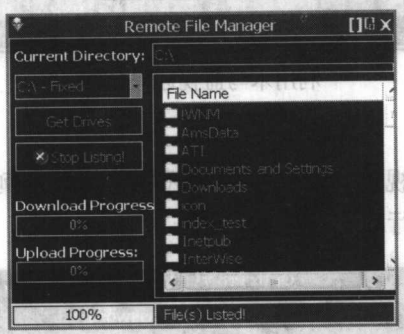
打开远程桌面监视

1-1-3 木马的功能

从网络上入侵一台计算机，并不是一件轻松的事，尤其是一些设防比较严密的系统，要找到系统漏洞入侵并不是十分容易的事，可能至少得花上几小时或数天时间。在成功入侵之后，黑客有时会使用木马程序，以便在需要时可以控制曾经入侵的系统。为了让黑客可以更方便地控制远程计算机，目前的木马程序通常会提供以下的功能：

- 远程文件管理功能。

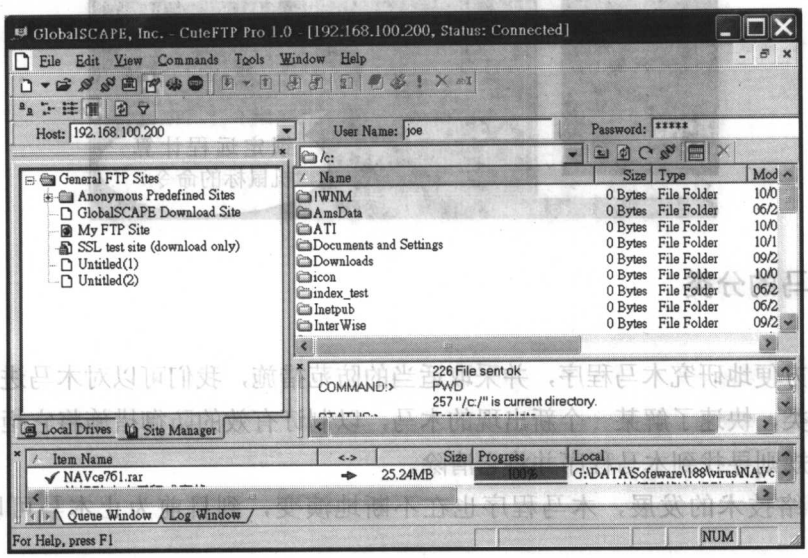
让黑客可以在连接远程计算机后，进行上传、下载或删除等文件管理操作。



利用木马 Optix Pro 管理远程计算机

- 打开常用网络服务。

为远程计算机安装常用的网络服务，让它为黑客或其他非法用户服务。



利用木马设定为 FTP 文件服务器后的计算机，可以提供 FTP 文件传输服务

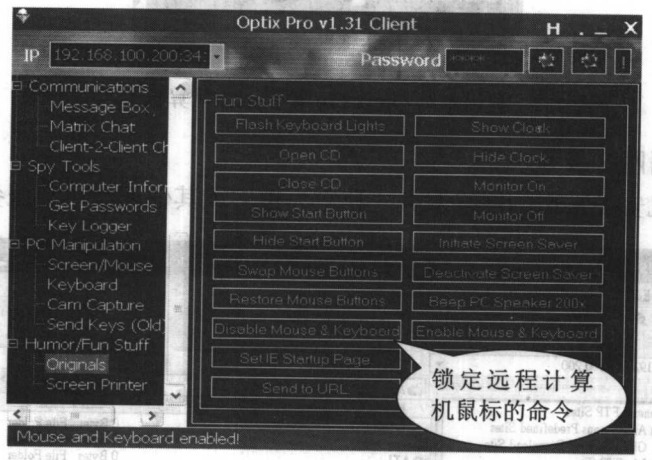
- 远程屏幕监视功能。

实时截取屏幕图像，以方便黑客实时监视远程用户目前正在进行哪些操作。

利用木马监视远程屏幕

- 控制远程计算机。

通过命令或通过远程监视窗口，直接控制远程计算机。例如在远程计算机执行程序、打开文件或向其他计算机进行攻击等。



1-1-4 木马的分类

为了更方便地研究木马程序，并采取适当的防范措施，我们可以对木马进行分类。并通过这些分类，快速了解某一个新出现的木马，以制订有效的防御措施将它拒之门外，或者通过一些规则寻找到木马程序并将它清除。

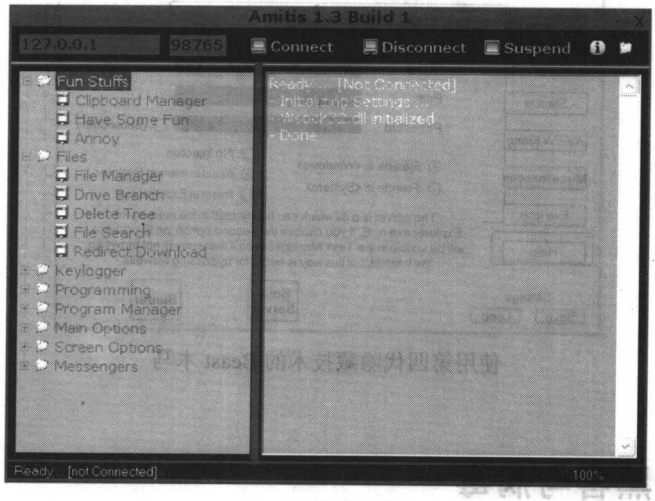
随着网络技术的发展，木马程序也在不断地演变，到目前为止木马可以分为以下四代：

- 第一代木马。

第一代木马出现在网络发展的早期，是以窃取网络密码为主要任务。随着第二代木马的出现，这种功能简单的木马基本上已经绝迹。

● 第二代木马。

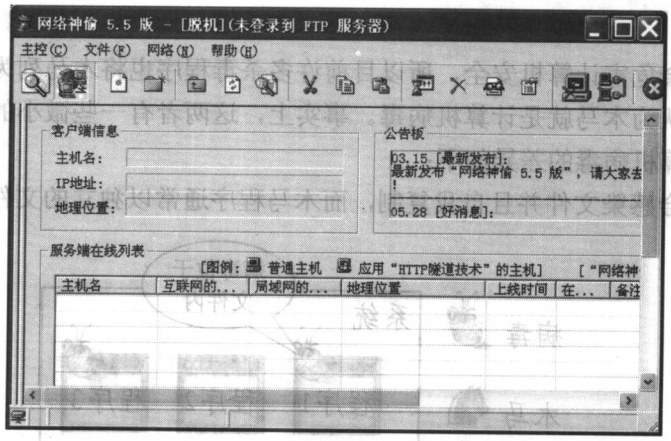
这是目前的主流，它使用标准的 C/S 架构，提供远程文件管理、屏幕监视等功能。但是由于植入木马的服务器程序，会打开连接端口等候客户端连接，因此比较容易被细心的用户发现。像“冰河”、Amitis 等都是典型的第二代木马程序。



Amitis 的客户端

● 第三代木马。

第三代木马在功能上与第二代没有太大差异，它的改变主要在网络连接方式上。它的特征是不打开连接端口进行侦听，使用 ICMP 通讯协议进行通讯或客户端在 80 等常用服务端口侦听，而服务器主动连接这些端口。不但用户难以察觉计算机已经被植入木马，就连防火墙也难以有效拦截。像网络神偷（Net thief）、Peep201 等都是典型的第三代木马程序。

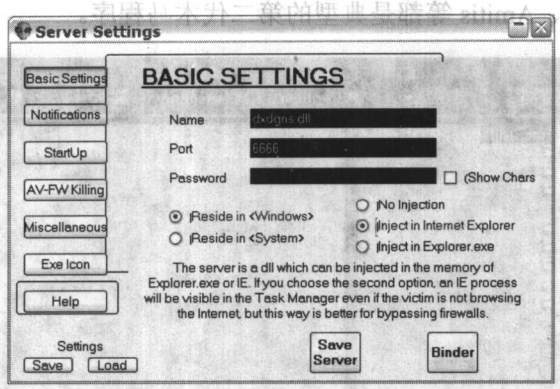


网络神偷

● 第四代木马。

前三代木马，大多都有独立的木马程序，因此用户可以根据启动项目中的描述内容，很快找到木马程序，并删除它。但是第四代木马在隐藏技术上，作了比较大的改变。选择

程序注册表的方式，以伪装成 DLL 文件的形式加载到正常的启动程序上，无法通过“任务管理器”查看到正在执行的木马。不过在连接方式上，依然使用第三代木马或第二代木马的连接方式。例如 Beast 就是典型的第四代木马程序。



使用第四代隐藏技术的 Beast 木马

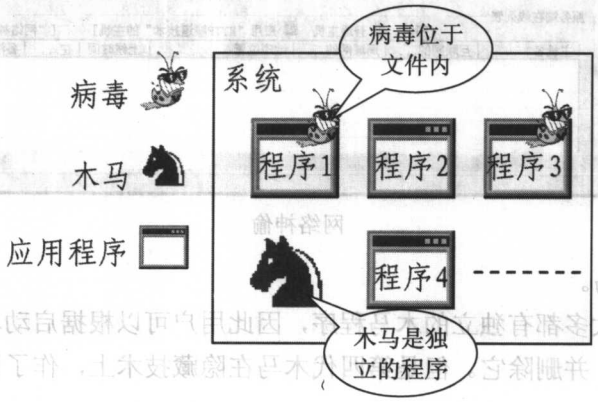
1-2 木马、黑客与病毒

经过第一节的介绍，相信大家对木马已经有了一个概略的了解。在使用计算机的过程中，所听到有关木马程序的信息，通常跟黑客、病毒联结在一起。究竟木马、黑客与病毒之间存在着什么样的关系？这一节将为大家解开这些疑惑。

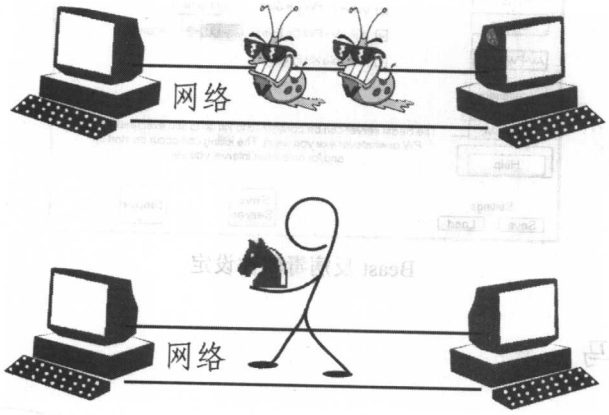
1-2-1 木马与病毒的区别与联系

由于木马也会危害计算机安全，所以目前许多杀毒程序也将木马列为扫除的范围，因此造成许多用户认为木马就是计算机病毒。事实上，这两者有一些微小的差异，不能划上等号，木马与计算机病毒的差异如下：

计算机病毒会感染文件并且自我复制，而木马程序通常以独立的文件存在，不会自我复制。

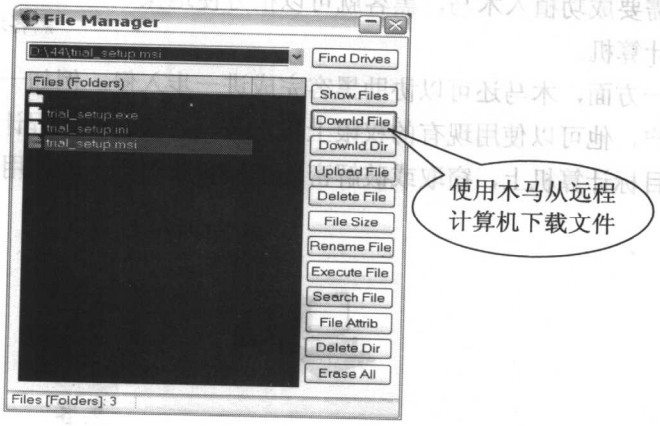


病毒会通过网络或其他方式主动入侵其他计算机，木马通常不会主动入侵计算机，而是由黑客放到受害者的计算机。



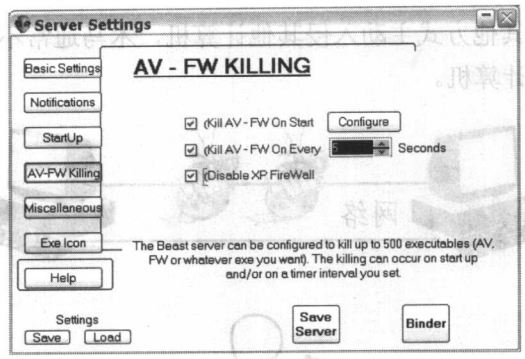
病毒与木马的入侵方式

病毒主要是破坏被入侵的计算机或恶作剧，而木马程序则是等候黑客连接，然后控制被入侵的计算机，窃取文件或进行监控。



当然随着病毒与木马编写技术的发展，这两者的差异正在不断缩小。例如一些蠕虫病毒，就会控制受感染的用户计算机，在指定的时间向事先确定的服务器发动攻击。而一些木马程序也不再乖乖遵守老一代木马程序的原则：加载—等候—完成远程命令，反而开始尝试利用系统漏洞，夺取系统管理员权限并为所欲为。目前相当多的新型木马程序，已经改变了以往躲避杀毒、防火墙软件的设计思维，变成主动出击，在执行后会立即关闭防火墙或杀毒软件。如果杀毒程序在一开始就无法识别这些木马，将会被木马压制而无法执行。例如木马程序 Beast，可以设定每隔 5 秒检测一次杀毒程序是否执行，如果执行就强行关闭。

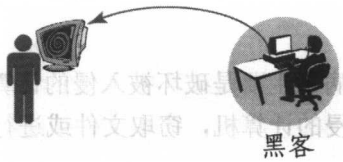
目前的病毒与木马这些恶意程序，还有合二为一的趋势，也就是在病毒上再带一个木马程序，然后在感染病毒的计算机中安装木马程序，这样黑客在很短时间内，就可以掌控许多计算机，进而对网络节点或大型网站发动攻击。



Beast 反病毒软件设定

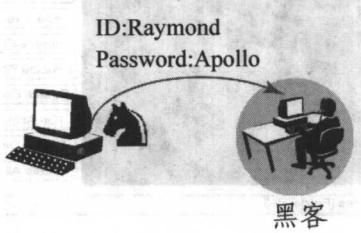
1-2-2 黑客与木马

从功能上而言，木马是一种体积小巧、执行隐密的程序。与从外面发动的攻击行为不同，木马程序会接收黑客的命令，操作以及控制计算机。因此，只需要成功植入木马，黑客就可以很方便地操控这台计算机。



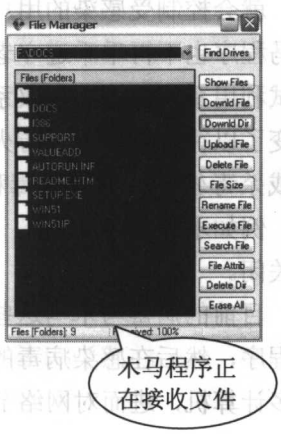
黑客通过木马控制远程计算机

另一方面，木马还可以协助黑客完成进一步入侵。例如一个黑客原本只有一个普通用户的帐户，他可以使用现有的权限上传木马，并让它在远程计算机上执行，然后木马就会潜伏在目标计算机上，窃取或破解密码让黑客获得更多的使用权限。



利用木马获得密码

由于木马能帮助黑客入侵网络上的其他计算机，因此许多黑客都喜欢使用木马程序。许多用户也将木马视为黑客的专用工具。事实上，木马就真的十恶不赦吗？其实也未必，因为除了一些具有恶意破坏功能的木马之外，许多木马事实上也是优秀的远程监控与传输工具，关键是看用户如何正确的使用。就如同利斧在凶犯手中是行凶的利器，而在伐木工人手中却是生财工具一样。（有关木马用于正途的问题，将在本书第 11 章中讨论）。



黑客之道：破解黑客木马屠城计

Chapter 2

闯进计算机的木马——木马对计算机的危害